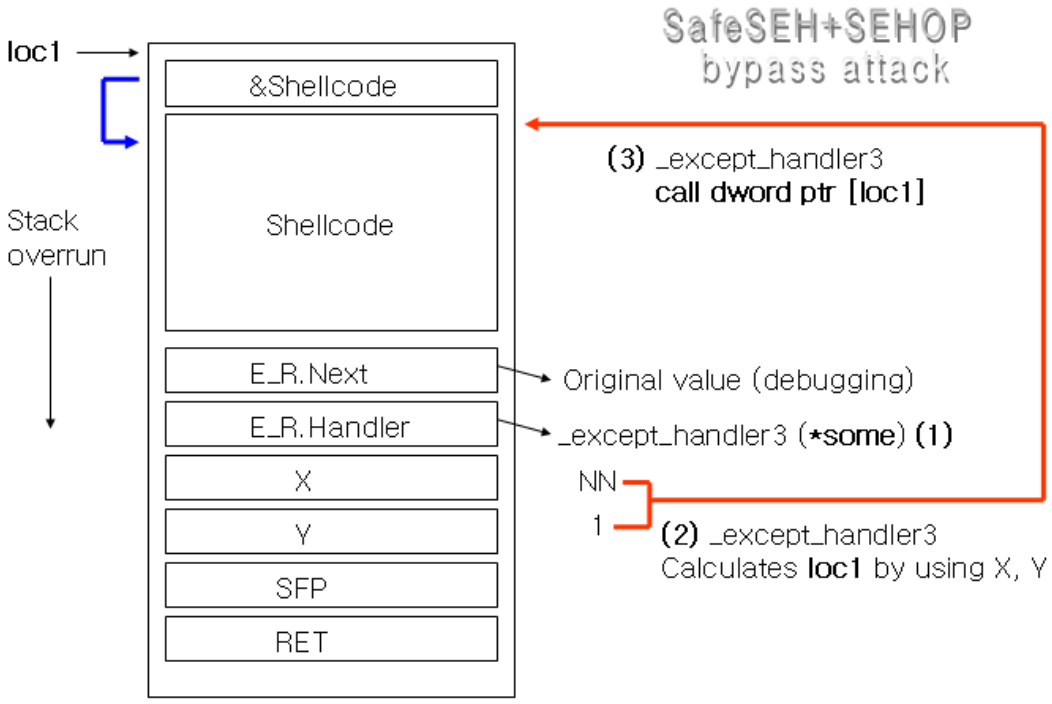
SafeSEH+SEHOP all-at-once bypass exploitation method principles

x90c

Jan 8. 2012

[Table of Contents]



*some windows system module's _except_handler3 hasn't any checking of user-defined Handler address(*loc1). Then we can use it for calling our shellcode indirectly.

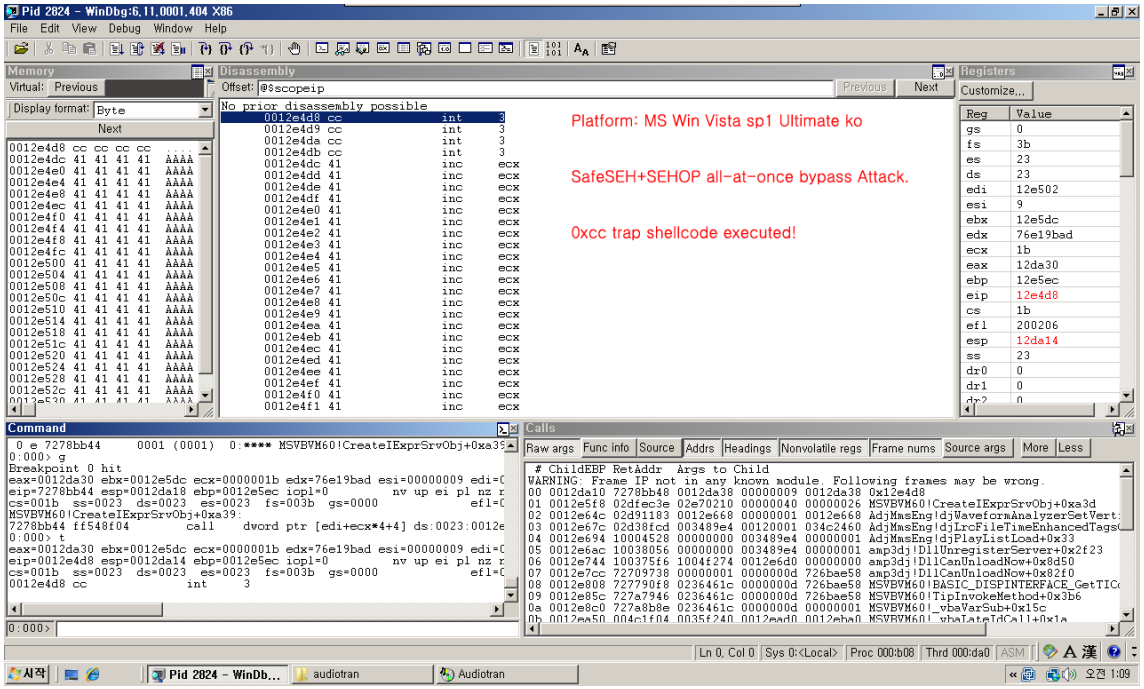
1. Which windows are SEHOP contained?

- Windows Vista sp1 (Optional)
- Windows 7 (Optional)
- Windows Server 2008 (Default enabled)
- Windows Server 2008 R2 (Default enabled) **[1]**

2. The exploitation method principles

There are two principles of SEHOP all-at-once bypass method.

1. Targeted(or victim) stackoverrun vulnerable application built by VC++ 6.0 and some other versions(non-tested).
2. The vulnerable application running on a box which SEHOP mitigation enabled windows environment.



3. Limitations

1. The method tested was with __except_handler3, not with __except_handler4.
2. The method tested was with not related with __EH4_CallFilterFunction of scopetable struct. It was using the SEH chain only.
3. The method was works by using __except_handler3-like copied routine around DLL's mapping area. (tested on Vista sp1 with SEHOP enabled manually.)
4. __except_handler4 also have the routine to call user-defined handler. then if you can, also abusing this. as __EH4_CallFilterFunction of ScopeTable abusing. after GS security cookie, EH security cookie checking (XORed). (some good references are exists on googling.)

4 Other mitigations?

- Stack ASLR In Vista sp1?

"*Microsoft's Windows Vista (released January 2007), Windows Server 2008, Windows 7, and Windows Server 2008 R2 have ASLR enabled by default,* although only for those executables and dynamic link libraries specifically linked to be ASLR-enabled.*[7]*
This did not include Internet Explorer 7 on Windows Vista prior to Service Pack 1; ASLR and Data Execution Prevention (DEP) are both disabled for application compatibility purposes." **[3]**

As you can see, Vista I tested only enabled for Executables and DLLs.
No Stack ASLR. and DEP is exists and can be applied to mapping areas.
Vista, Windows Server 2008, Windows 7 is the SEHOP systems.

But if you want to enable stack ASLR on Vista. then it's also able to do.

"When executing a program whose image has been marked for ASLR, the memory layout of the process is further randomized *by placing the thread stack and the process heaps randomly.*" **[4]**

As you may know, Process Heaps also can be ramdomized.

- DEP?

The method was not considered about DEP(Data Execution Prevention).

5. References

[1] http://support.microsoft.com/kb/956607
[2] http://support.microsoft.com/kb/956607/en
[3] http://en.wikipedia.org/wiki/Address_space_layout_randomization
[4] http://www.symantec.com/avcenter/reference/Address_Space_Layout_Randomization.pdf
[5] AudioTran 1.4.2.4 SafeSEH+SEHOP Exploit. http://www.exploit-db.com/exploits/15184